



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/044,019	01/11/2002	Partha Bhattacharya	50325-0629	8175
29989	7590	11/26/2008	EXAMINER	
HICKMAN PALERMO TRUONG & BECKER, LLP			MOORTHY, ARAVIND K	
2055 GATEWAY PLACE				
SUITE 550			ART UNIT	PAPER NUMBER
SAN JOSE, CA 95110			2431	
			MAIL DATE	DELIVERY MODE
			11/26/2008	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/044,019	BHATTACHARYA ET AL.
	<b>Examiner</b>	<b>Art Unit</b>
	Aravind K. Moorthy	2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 29 July 2008.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 10,11,14-16 and 33-48 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 10,11,14-16 and 33-48 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 27 October 2003 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ .                                    |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____.   | 6) <input type="checkbox"/> Other: _____ .                        |

## **DETAILED ACTION**

1. This is in response to the amendment filed on 29 July 2008.
2. Claims 10, 11, 14-16 and 33-48 are pending in the application.
3. Claims 10, 11, 14-16 and 33-48 have been rejected.
4. Claims 1-9, 12, 13, 17-32 and 49-52 have been cancelled.

### ***Response to Arguments***

5. Applicant's arguments with respect to claims 10, 11, 14-16 and 33-48 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. **Claims 10, 11, 33-41 and 45-48 are rejected under 35 U.S.C. 102(b) as being anticipated by Caronni et al U.S. Patent No. 5,761,669 (hereinafter Caronni).**

As to claim 10, Caronni discloses a method as recited, wherein identifying one or more first sub-entries in the first access control list comprises:

identifying a dimensional range and a policy action for each entry in the first access control list [column 4, lines 23-35];  
identifying all overlapping dimensional ranges in the first access control list, each overlapping dimensional range corresponding to where the dimensional

ranges of entries in the first access control list overlap [column 7 line 51 to column 8 line 13];

identifying all non-overlapping dimensional ranges in the first access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the first access control list that do not overlap dimensional ranges of other entries in the first access control list [column 7 line 51 to column 8 line 13];

identifying a policy action for each identified overlapping dimensional range in the first access control list [column 7 line 51 to column 8 line 13]; and

identifying a policy action for each identified non-overlapping dimensional range of the first access control list [column 7 line 51 to column 8 line 13].

As to claims 11 and 41, Caronni discloses as recited, wherein identifying second sub-entries in the second access control list comprises:

identifying a dimensional range and a policy action for each entry in the second access control list [column 7, lines 1-39];

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap [column 7, lines 1-39];

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to

dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list [column 7, lines 1-39];

identifying a policy action for each identified overlapping dimensional range of the second access control list [column 7, lines 1-39]; and

identifying a policy action for each identified non-overlapping dimensional range of the second access control list [column 7, lines 1-39].

As to claim 33, Caronni discloses a method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:

subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and the another control entry are two access control entries of multiple first access control entries and wherein the first access control entries, including the particular access control entry and the another access control entry, are all of access control entries as specified in a first access control list [abstract, column 7 line 51 to column 8 line 13];

identifying one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one of the one or more first sub-entries is derived from results of subtracting the particular access control entry from the another access control entry [abstract, column 7 line 51 to column 8 line 13]; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by one or more entries of multiple second access control entries the second access control list [abstract, column 7 line 51 to column 8 line 13].

As to claims 34, 38 and 46, Caronni discloses determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is contained by one or more entries of the second access control list [column 7, lines 21-27].

As to claims 35, 39 and 47, Caronni discloses a method as recited, further comprising:

identifying second sub-entries in the second access control list, wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries [column 8, lines 30-55]; and

wherein determining whether each of the first sub-entry in the first access control list is contained by one or more entries of the second access control list includes determining whether the each of the first sub-entries in the first access control list is contained by one or more of the second sub-entries identified from the second control list [column 8, lines 30-55].

As to claim 36, Caronni discloses a computer readable medium for comparing access control lists to configure a security policy on a network, the computer readable medium carrying instructions for performing the steps of:

Subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and the another control entry are two access control entries multiple first access control entries and wherein the first access control entries, including the particular access control entry and the another access control entry, are all of access control entries as specified in a first access control list [abstract, column 7 line 51 to column 8 line 13];

identifying one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one of the one or more first sub-entries is derived from results of subtracting the particular access control entry from the another access control entry [abstract, column 7 line 51 to column 8 line 13]; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by one or more entries of multiple second access control entries in the second access control list [abstract, column 7 line 51 to column 8 line 13].

As to claim 37, Caronni discloses a policy server communicatively coupled to security devices in a network to configure a security policy on a network, the policy server comprising:

- a processor [column 3, lines 32-47];
- a network interface that communicatively couples the processor to the network to receive flows of packets therefrom [column 3, lines 32-47];
- a memory [column 3, lines 32-47]; and
- sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out the steps of:
  - subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and the another control entry are two access control entries multiple first access control entries and wherein the first access control entries, including the particular access control entry and the another access control entry, are all of access control entries as specified in a first access control list [abstract, column 7 line 51 to column 8 line 13];
  - identifying one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one of the one or more first sub-entries is derived from results of subtracting the particular access control entry from the another access control entry [abstract, column 7 line 51 to column 8 line 13]; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by one or more entries of multiple second access control entries in the second access control list [abstract, column 7 line 51 to column 8 line 13].

As to claims 40 and 48, Caronni discloses a policy server as recited, wherein the instructions for performing identifying one or more first sub-entries in the first access control list comprise:

instructions for performing identifying a dimensional range and a policy action for each entry in the second access control list [column 8, lines 30-55];

instructions for performing identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap [column 8, lines 30-55];

instructions for performing identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list [column 8, lines 30-55];

instructions for performing identifying a policy action for each identified overlapping dimensional range in the second access control list [column 8, lines 30-55]; and

instructions for performing identifying a policy action for each identified non-overlapping dimensional range of the second access control list [column 8, lines 30-55].

As to claim 45, Caronni discloses an apparatus for comparing access control lists to configure a security policy on a network, the apparatus comprising:

means for subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and the another control entry are two access control entries multiple first access control entries and wherein the first access control entries, including the particular access control entry and the another access control entry, are all of all of access control entries as specified in a first access control list [abstract, column 7 line 51 to column 8 line 13];

means for identifying based one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one or more first sub-entries is derived from results of subtracting the particular access control entry from the another access control entry [abstract, column 7 line 51 to column 8 line 13]; and

means for programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by

one or more entries of multiple second access control entries the second access control list [abstract, column 7 line 51 to column 8 line 13].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**7. Claims 14 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caronni U.S. Patent No. 5,761,669 as applied to claims 33, 37 and 45 above, and further in view of Brawn et al U.S. Patent No. 7,020,718 B2.**

As to claims 14 and 42, Caronni does not teach that identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

Brawn et al teaches identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list [column 8 line 41 to column 9 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Caronni so that a dimensional range and a policy action would have been identified for each entry in the first access control list that would have

included identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Caronni by the teaching of Brawn et al because an advantage includes providing a discontiguous address plan that allows thousands of discrete, different sized, and seemingly irregularly spaced address ranges to be accessed and identified by a small number of address and mask combinations. Another advantage includes providing an enterprise having a large complex network with a discontiguous network address plan configured to optimize for route advertisement, ACL entries, firewall configurations, and multiple network policies [column 6, lines 27-35].

**8. Claims 15 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caronni U.S. Patent No. 5,761,669 as applied to claims 33, 37 and 45 above, and further in view of Mate et al U.S. Patent No. 7,020,718 B2.**

As to claims 15 and 43, Caronni does not teach that identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

Mate et al teaches identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list [column 11, lines 4-19].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Caronni so that a dimensional range and a policy

action would have been identified for each entry in the first access control list that would have included identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Caronni by the teaching of Mate et al because it provides a method and system having fast search capabilities for classifying a plurality of types of data traffic and route lookup [column 3, lines 14-16].

**9. Claims 16 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caronni U.S. Patent No. 5,761,669 as applied to claims 33, 37 and 45 above, and further in view of Banginwar U.S. Patent No. 7,020,718 B2.**

As to claims 16 and 44, Caronni does not teach identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

Banginwar teaches identifying a communication protocol for communication packets specified by each of the entries in the first access control list [column 3, lines 18-46].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Caronni so that a dimensional range and a policy action would have been identified for each entry in the first access control list that would have included identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Caronni by the teaching of Banginwar because it enables a policy manager to communicate with the many devices connected to it [column 3, lines 47-54].

***Conclusion***

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/  
Examiner, Art Unit 2431

/Christopher A. Revak/  
Primary Examiner, Art Unit 2431